REMARKS

In the non-final Office Action, the Examiner rejects claims 34-50 under 35 U.S.C. § 101 as directed to non-statutory subject matter; and rejects claims 1-50 under 35 U.S.C. § 102(b) as anticipated by COLEY et al. (U.S. Patent No. 5,826,014). Applicants respectfully traverse the rejections under 35 U.S.C. § 101 and 102 with respect to the claims, as currently presented.

By the present amendment, Applicants cancel claim 43 without prejudice or disclaimer and amend claims 34 and 44 to improve form. No new matter has been added by way of the present amendment. Claims 1-42 and 44-50 remain pending.

As an initial matter, Applicants filed Information Disclosure Statements on October 21, 2002 and October 6, 2003. With respect to the Information Disclosure Statement, filed October 21, 2002, Applicants note that several documents submitted with the Information Disclosure Statement (documents M-EE) were not considered by the Examiner. Moreover, the Examiner does not explain why these documents were not considered. Applicants respectfully request that these documents be properly considered and that the attached Form-1449 be initialed and returned to Applicants or an explanation be given as to why these documents are not being considered.

With respect to the Information Disclosure Statement, filed October 6, 2003, one of the documents submitted with the Information Disclosure Statement, namely Barrett et al., "Intermediaries: New Places for Producing and Manipulating Web Content," Computer Networks and ISDN Systems 30, 1998, pp. 509-518, was not properly

considered. Applicants respectfully request that this document be properly considered and that the attached Form-1449 be initialed and returned to Applicants.

Pending claims 34-42 and 44-50 stand rejected under 35 U.S.C. § 101 as allegedly directed to non-statutory subject matter. In particular, the Examiner alleges "[t]he computer readable medium in claims 34 and 44 is explained in the specification as including a carrier wave. A carrier wave is not a tangible medium and is therefor non-statutory. The computer readable medium must be recordable for it to satisfy the requirements of statutory subject matter" (Office Action, pg. 2). Applicants amend claims 34 and 44 to identify the computer readable medium as tangible. Therefore, Applicants respectfully request that the rejection of claims 34 and 44 (and their dependent claims) under 35 U.S.C. § 101 be reconsidered and withdrawn.

Pending claims 1-42 and 44-50 stand rejected under 35 U.S.C. § 102(b) as allegedly anticipated by COLEY et al. Applicants respectfully traverse this rejection with respect to the claims as currently presented.

A proper rejection under 35 U.S.C. § 102 requires that a single reference teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. See M.P.E.P. § 2131. COLEY et al. does not disclose the combination of features recited in claims 1-50.

For example, independent claim 1 is directed to a method for accessing resources on a private network via an intermediary server. The method includes receiving a login request from a user for access to the intermediary server; authenticating the user; subsequently receiving a resource request from the user at the intermediary server, the

resource request requesting a particular operation with respect to a resource from the private network; obtaining access privileges for the user; determining whether the access privileges for the user permit the user to perform the particular operation at the private network; and preventing performance of the particular operation at the private network such that a response to the resource request is not had when said determining (e) determines that the access privileges for the user do not permit the user to perform the particular operation at the private network. COLEY et al. does not disclose or suggest this combination of features.

For example, COLEY et al. does not disclose or suggest receiving a login request from a user for access to an intermediary server. The Examiner relies on col. 10, line 1, to col. 11, line 31, of COLEY et al. for allegedly disclosing this feature (Office Action, pg. 3). Applicants respectfully disagree with the Examiner's interpretation of COLEY et al.

At col. 10, line 1, to col. 11, line 31, COLEY et al. discloses a test that can be performed by a proxy agent in a firewall device in response to receiving a request for access to a destination device. The test involves checking whether the destination address indicated by an access request is authorized. This section of COLEY et al. also discloses that when the proxy agent successfully completes its set of verification tests, the proxy agent initiates a connection request to the destination device. This section of COLEY et al. in no way discloses or suggests receiving a login request from a user for access to an intermediary server, as required by claim 1.

COLEY et al. discloses a user accessing a destination device through a proxy agent in a firewall device. Thus, Applicants assume the Examiner alleges that the proxy agent (or firewall device) corresponds to the intermediary server recited in claim 1. With this interpretation in mind, COLEY et al. in no way discloses or suggests receiving a login request from a user for access to a proxy agent (or firewall device), as would be required by the Examiner's interpretation of claim 1. Instead, COLEY et al. merely discloses that the proxy agent acts to restrict access to destination devices (see, for example, col. 5, lines 49-64).

The Examiner has not pointed to any section of COLEY et al. that discloses receiving a login request from a user for access to an intermediary server, as required by claim 1. Therefore, a proper case of anticipation has not been established with respect to claim 1.

For at least the foregoing reasons, Applicants submit that claim 1 is not anticipated by COLEY et al.

Claims 2-18 depend from claim 1. Therefore, these claims are not anticipated by COLEY et al. for at least the reasons given above with respect to claim 1. Moreover, these claims recite additional features not disclosed or suggested by COLEY et al.

For example, claim 3 recites that the authenticating determines whether the user is authenticated based on an external authentication server. The Examiner relies on col. 8, lines 42-61, of COLEY et al. for allegedly disclosing this feature (Office Action, pg. 4). Applicants respectfully disagree with the Examiner's interpretation of COLEY et al.

At col. 8, lines 42-61, COLEY et al. discloses:

> The firewall 318 permits the internal network 328 to be attached to the public network 306 (through the publicly accessible network 312) without rendering the secure network 328 open to public access. The firewall 318, in accordance with preferred embodiments of the invention, physically separates the publicly accessible network 312 from the internal network 328. Consequently, all communications attempting to access the internal network 328, or any network elements attached thereto, must pass through the firewall 318. To secure it from direct (i.e., keyboard) access, the firewall 318 is preferably maintained in a secure location on the premises of the institution 310.
>
> The firewall 318 can run on a general purpose computer. Such a computer, in accordance with preferred embodiments, is a stand alone machine, or firewall box, dedicated to the firewall application. The addition of other programs to the firewall box merely undermines the strength of the firewall 318. Such additional programs can be used to bypass, or attach to and attack the firewall 318.

This section of COLEY et al. discloses that firewall 318 resides between an internal network 328 and a public network 306. This section of COLEY et al. in no way discloses or suggests determining whether the user is authenticated based on an external authentication server, as required by claim 3. In fact, this section of COLEY et al. seems to teach away from the use of an external authentication server since such an external device could be used to attack the firewall, as COLEY et al. suggests.

For at least these additional reasons, Applicants submit that claim 3 is not anticipated by COLEY et al.

Claim 4 recites that the external authentication server is within the private network. Since, as set forth above with respect to claim 3, COLEY et al. does not disclose or suggest an external authentication server, COLEY et al. cannot disclose or suggest an external authentication server that is within a private network, as required by claim 4.

The Examiner relies on col. 8, lines 42-54, of COLEY et al. for allegedly disclosing this feature (Office Action, pg. 5). Applicants respectfully disagree with the Examiner's interpretation of COLEY et al.

Col. 8, lines 42-54, of COLEY et al. is reproduced above. This section of COLEY et al. discloses that firewall 318 resides between an internal network 328 and a public network 306. This section of COLEY et al. in no way discloses or suggests an external authentication server that is within a private network, as required by claim 4. In fact, this section of COLEY et al. seems to teach away from the use of an external authentication server since such an external device could be used to attack the firewall, as COLEY et al. suggests.

For at least these additional reasons, Applicants submit that claim 4 is not anticipated by COLEY et al.

Independent claim 19 recites features similar to (yet possibly of different scope than) features recited above with respect to claim 1. Therefore, Applicants submit that claim 19 is not anticipated by COLEY et al. for at least reasons similar to reasons given above with respect to claim 1.

Claims 20-30 depend from claim 19. Therefore, these claims are not anticipated by COLEY et al. for at least the reasons given above with respect to claim 19. Moreover, these claims recite additional features not disclosed or suggested by COLEY et al.

For example, claim 20 recites that supplying the particular resource to the remote user includes retrieving the particular resource from a content server, modifying at least

one URL within the particular resource, and sending the modified resource to the remote user. COLEY et al. does not disclose or suggest this combination of features.

For example, COLEY et al. does not disclose or suggest modifying at least one URL within the particular resource and sending the modified resource to the remote user. The Examiner relies on col. 11, lines 1-40, of COLEY et al. for allegedly disclosing these features (Office Action, pg. 8). Applicants respectfully disagree with the Examiner's interpretation of COLEY et al.

At col. 11, lines 1-40, COLEY et al. discloses:

> To access the Web server of the institution 310, the user 300 enters an appropriate address (step 402), such as "http://webwho.com". The access request is received by a router 304 which forwards the message to the Internet 306. The Internet may forward the message through a series of routers and present it to a router 308 that services the institution 310.
>
> Because the access request seeks to access a destination address residing behind the firewall 318, the access request message is presented to the firewall 318 (step 404). In accordance with an exemplary embodiment, a proxy agent running on the firewall 318 is assigned to the access request in accordance with a preliminary analysis of the port number designation within the packet representing the access request (step 406). In this case, port number 80 (HTTP) would ordinarily be designated in the request. The assessment also can involve a determination of whether the service indicated by the port number comports with the contents of the request (step 408). That is, does the request indicate one service (port number) while being formatted for another. If there is disparity, the access is denied (step 410).
>
> The proxy agent can then analyze a source address to determine whether the host computer 302 from which the message originated is authorized to access the secure Web server 322 (step 412). As described above, this check can be used to optionally invoke a more rigorous set of verification checks if the source is unknown or suspect. This assessment can involve a comparison of the source address with a list of authorized or unauthorized addresses maintained by the proxy agent (step 414). In the exemplary case here, if the source address is not authorized (i.e., the source address is not

> on the list), the access request is denied (step 416). The extent to which a proxy agent verifies the validity of an access request can vary. It should be noted that in some cases, a proxy agent may need do little more than verify address information before initiating a connection to the destination device on behalf of the source host. Alternatively, if a source address is suspect, or a proxy agent's set of checks is fixed, the proxy agent can perform additional checking.

This section of COLEY et al. discloses the proxy agent determining whether to grant access to a destination device based on the source address of the host computer that sent the access request. This section of COLEY et al. in no way discloses or suggests the proxy agent or any other device modifying at least one URL within the particular resource and sending the modified resource to the remote user, as required by claim 20.

If this rejection is maintained, Applicants respectfully request that the Examiner explain how the above section of COLEY et al. can reasonably be construed to disclose modifying at least one URL within the particular resource and sending the modified resource to the remote user, as required by claim 20.

For at least these additional reasons, Applicants submit that claim 20 is not anticipated by COLEY et al.

Claim 21 recites that supplying the particular resource to the remote user includes modifying the response so that links within the response point to the intermediate server and sending the modified resource to the remote user. The Examiner relies on col. 8, lines 64-67, col. 9, lines 1-31, col. 10, lines 1-26, and col. 12, lines 6-24, of COLEY et al. for allegedly disclosing these features (Office Action, pg. 8). Applicants respectfully disagree with the Examiner's interpretation of COLEY et al.

At col. 8, line 64, to col. 9, line 1, COLEY et al. discloses:

> A proxy agent is preferably assigned in accordance with a port number designation indicated in a request. The assigned proxy agent processes the access request, forms the connection, if verified, and manages the completed connection.

This section of COLEY et al. discloses that a proxy agent forms and manages connections. This section of COLEY et al. in no way discloses or suggests modifying a response so that links within the response point to the intermediate server and sending the modified resource to the remote user, as required by claim 21.

At col. 9, lines 1-31, COLEY et al. discloses:

> A designer can dictate what set of verification tests are to be run on a particular incoming request. For instance, an assigned proxy agent can first check to ensure that the protocol of the access request matches that of the indicated port. If there is a discrepancy, the request is denied. A next check can involve investigation of a source address (i.e., the host machine from which the access inquiry originated) of the access request. This permits the proxy agent to make an initial assessment of the authenticity of the request. If a particular source has a higher probability of generating suspect packets (e.g., an unknown university computer) a proxy agent can optionally invoke a more rigorous series of verification tests. However, if the source is inherently secure (e.g., a firewall protected machine at a company's headquarters communicating with their R&D site) the proxy agent might proceed directly to connecting the incoming request with a destination host machine. Once the source is determined, the proxy agent can run an appropriate combination of verification checks suited to the integrity of the request as indicated by its source. In the event that a legitimate user is accessing a protected network element using suspect computer (e.g., a visiting professor logging on to a university's host computer rather than his or her office computer) it may be advantageous to allow such a user through, but only after a more rigorous set of interactive verification tests. However, the packet source address need not necessarily dictate the particular combination of verification tests performed by the proxy agent. A proxy agent can have a fixed set of verification tests based on the port designation. The particular selection of verification checks is discretionary. Several such checks are described below.

This section of COLEY et al. discloses that a proxy agent can perform a number of verification checks. This section of COLEY et al. in no way discloses or suggests modifying a response so that links within the response point to the intermediate server and sending the modified resource to the remote user, as required by claim 21.

At col. 9, line 67, to col. 10, line 27, COLEY et al. discloses:

> The time period check can include any combination of time of day, day of week, week of month, month of year, and/or year.
>
> A fourth check can be invoked to determine whether the destination address indicated by an access request is authorized. This check can be performed by examining packet destination address information, or possibly by prompting a user to enter the information. For example, in File Transfer Protocol (FTP) requests, the user may be required to enter the destination address (e.g., "username@host") in response to a prompt generated by the assigned proxy agent.
>
> A proxy agent can also run tests that intercept and discard any messages that attempt to initiate a process on the firewall 318 itself. For example, a conventional system having bundled applications may include an application such as SendMail. SendMail, in addition to providing mail delivery, also contains features for collecting and tracking source and destination information of mail messages. The information derived by a hacker through execution of such SendMail commands can be used to gain access to secure network elements. Hence, a proxy agent in accordance with the invention can include, within its set of tests, a check for ferreting out and discarding packets having nested executable commands. A firewall incorporating the invention can, however, facilitate the communication of normal electronic messages. Hence, valid mail can be passed through the firewall 318 to an internal E-mail system 320 if otherwise authorized.

This section of COLEY et al. discloses that a proxy agent can perform a verification check based on the destination address and that the proxy agent can intercept and discard any messages that attempt to initiate a process on firewall 318. This section of COLEY et al. in no way discloses or suggests modifying a response so that links within the response

point to the intermediate server and sending the modified resource to the remote user, as required by claim 21.

At col. 12, lines 6-24, COLEY et al. COLEY et al. discloses:

> If after the proxy agent has completed its set of tests it is determined that the access request is authorized, the proxy agent initiates a connection to the Web server 322 on behalf of the source machine 300 (step 440). Because the firewall forms a connection (using a proxy agent) following the completion of validation checks associated with the proxy agent's test set, the firewall functions as a Bastion host, or firewall server, on behalf of the access request source. By using the firewall as a Bastion host, or firewall server, to act on behalf of the user accessing the secure network 328, the identity of internal network elements is not revealed because the firewall 318, acting as an intermediary, shields the identity of the network elements for whom it is acting on behalf of. All the external user sees, in terms of addresses, is the firewall. If an internal connection is tapped onto, a valid source address or user identity is not available to the hacker as the firewall 318 appears to be the source of the connection. Hence, a firewall arrangement in accordance with the invention provides two-way transparency.

This section of COLEY et al. discloses that a proxy agent can act a Bastion host, or firewall server, on behalf of the access request source. This section of COLEY et al. in no way discloses or suggests modifying a response so that links within the response point to the intermediate server and sending the modified resource to the remote user, as required by claim 21. This section of COLEY et al. in no way discloses or suggests modifying links within a response.

For at least these additional reasons, Applicants submit that claim 21 is not anticipated by COLEY et al.

Independent claim 31 recites features similar to (yet possibly of different scope than) features described above with respect to claims 1, 20, and 21. Therefore,

Applicants submit that claim 31 is not anticipated by COLEY et al. for at least reasons similar to reasons given above with respect to claims 1, 20, and 21.

Claims 32 and 33 depend from claim 31. Therefore, these claims are not anticipated by COLEY et al. for at least the reasons given above with respect to claim 31.

Independent claims 34 and 44 recite features similar to (yet possibly of different scope than) features recited above with respect to claim 1. Therefore, Applicants submit that claims 34 and 44 are not anticipated by COLEY et al. for at least reasons similar to reasons given above with respect to claim 1.

Claims 35-42 depend from claim 34. Therefore, these claims are not anticipated by COLEY et al. for at least the reasons given above with respect to claim 34. Moreover, these claims recite additional features not disclosed or suggested by COLEY et al.

For example, claim 36 recites a feature similar to (yet possibly of different scope than) a feature described above with respect to claim 3. Therefore, Applicants submit that claim 36 is not anticipated by COLEY et al. for at least reasons similar to reasons given above with respect to claim 3.

Claims 45-50 depend from claim 44. Therefore, these claims are not anticipated by COLEY et al. for at least the reasons given above with respect to claim 44. Moreover, these claims recite additional features not disclosed or suggested by COLEY et al.

For example, claims 45 and 46 recite features similar to (yet possibly of different scope than) features described above with respect to claims 20 and 21. Therefore, Applicants submit that claims 45 and 46 are not anticipated by COLEY et al. for at least reasons similar to reasons given above with respect to claims 20 and 21.

In view of the foregoing amendments and remarks, Applicants respectfully request the Examiner's reconsideration of this application, and the timely allowance of the pending claims.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY SNYDER, LLP

By: _____
John E. Harrity
Reg. No. 43,367

Date: April 3, 2006

11350 Random Hills Road
Suite 600
Fairfax, Virginia 22030
(571) 432-0800